# September 11th Report Card – Senator Charles E. Schumer

September 4, 2006

## Port Security

GRADE: D

*"While commercial aviation remains a possible target, terrorists may turn their attention to other modes. Opportunities to do harm are as great, or greater, in maritime and surface transportation." (9/11 Commission)*

After the 9/11 attacks revealed to the nation that seaports around the country were an easy access point for terrorists to smuggle a nuclear weapon into the United States, the government moved to strengthen port security by setting specific requirements for perimeter protection and employee identification, expanding customs screening programs in the United States and around the world, and developing advanced rapid nuclear screening technology for cargo. Unfortunately, five years later, none of these goals have been fully achieved.

- **Cargo screening technology is outdated and unlikely to catch a nuclear weapon.** According to Steven Flynn, a port security expert at the Council on Foreign Relations, "the radiation-detection technology currently used in the world's ports by the Coast Guard and Customs and Border Protection Agency is not adequately capable of detecting a nuclear weapon or a lightly shielded dirty bomb. This is because nuclear weapons are extremely well-shielded and give off very little radioactivity. If terrorists obtained a dirty bomb and put it in a box lined with lead, it's unlikely radiation sensors would detect the bomb's low levels of radioactivity."

- **There is still no standard biometric, tamperproof identification card for port workers and truck drivers who access seaport areas.** DHS reported that identity cards, already distributed to thousands of truckers by the Port Authority of New York and New Jersey, had been issued with virtually no background checks. The report found that of the 9,000 truckers checked, nearly half had evidence of criminal records. More than 500 held false or invalid driver's licenses.

- **Right now, only 5 percent of containers shipped into the United States are manually inspected**. This leaves more than ten million cargo containers that enter the United States without any thorough, hands-on inspection.

- **Millions of containers that are shipped to the United States do not have tamper-proof seals and locks to let security officials know whether a container has been opened since it was filled.** The Department of Homeland Security has failed to develop the standards for cargo locks and seals that were due to Congress on January 1, 2004. A DHS study, released earlier this year, found that "most containers are sealed with mechanical bolts that can be cut and replaced or have doors that can be removed by dismantling hinges."

- **DHS's current system to target high-risk cargo is like finding a needle in a haystack and we are spending more time looking through lemons and laundry detergent than searching for nuclear weapons.** DHS designated two worldwide programs to pick out high risk cargo and vet foreign shippers, the Container Security Initiative (CSI) and the Customs Trade Partnership Against Terrorism (C-TPAT). Unfortunately, as with port security as a whole, these programs are under-funded and poorly managed.

C-TPAT relies primarily on the "pledge" of shippers to send the only "legitimate cargo," rather than having customs agents validate security for these shippers.

Critics of the CSI program point out that while the program has merit, several factors limit the ability of Customs and Border Patrol (CBP) to police containers effectively. Staff shortages at foreign ports, operational limitations, and the lack of specific requirements for equipment and inspections leads to doubts about the ability of the CSI program to detect weapons of mass destruction (WMD) in shipping containers. After arrival in the United States, containers are transferred into the equally insecure world of domestic trucking.

- **Funding devoted to beef up port security is 95 percent less than funding dedicated to airport security.** To date, Congress has allocated only $878 million to help local officials improve physical security at ports, but we've spent more than $18 billion on aviation security. By the end of September 2006, DHS will have provided $876 million in Port Security Grant funds since 9/11, which is only about 20 percent of the $4.35 billion in federal assistance identified and applied for in six rounds of Port Security Grants.

## Mass Transit Security

GRADE: F

*"While the foiled terrorist plot to use liquid explosives to blow up airliners bound from Britain to the United States has again focused attention on terrorism in the skies, action also is needed to increase security on a far more vulnerable form of mass transit: commuter trains, subways and buses." (Peter Chalk, RAND Corporation)*

Mass transit systems have been a prime target for terrorists for decades. Yet prior to 9/11, subways, buses, and long distance trains in New York and across the country were left woefully unprotected. Despite the obvious threat, many stations were not equipped with closed-circuit security camera systems and bomb detectors were only deployed in extraordinary circumstances.

In the wake of the 9/11 attacks, local and federal law enforcement stepped up police presence at stations and deployed bomb-sniffing dog teams, but other than that, there was no advanced technology available to immediately detect the presence of a nuclear, biological, chemical, or explosive device. DHS has only issued voluntary security guidelines for transit operators. Currently, bomb detection technology is still in the early testing phases and is too slow to be used on busy systems.

- **Five years after 9/11, research and development into new explosive, radiological, chemical, and biological detectors is still in the early developmental stages.** TSA created a mass transit security pilot program in 2004 called the Transit and Rail Inspection Pilot (TRIP). Though TSA has another testing program underway in New Jersey, no system is fully operational. In addition, even after train bombings in Madrid, London, and Mumbai, TSA did not mandate that rail or mass transit systems install technology that could detect explosive devices.

- **TSA does not currently have the personnel to adequately ensure the security of our nation's rail and mass transit systems.** In contrast to the roughly 43,000 aviation screeners, there are only 100 surface inspectors. These inspectors are charged with covering more than 300,000 of freight rail lines, which are also used by Amtrak passenger trains, and 10,000 miles of commuter and subway rail lines.

- **Five years after 9/11, DHS still has not issued mandatory security requirements to protect transit systems.** In May 2004, DHS issued a number of voluntary directives which called on major transit operators to enhance physical security by, among other measures, installing transparent bomb-resistant trash cans, deploying additional police and security personnel, and installing closed-circuit security cameras. DHS has done little to ensure that these directives have been followed even after the bombings in Madrid, London, and Mumbai.

- **Even though two of the last three major mass transit attacks occurred on above ground, longer distance commuter lines, Amtrak and regional commuter rail systems remain woefully unprotected.** According to a March 2006 report by the Government Accountability Office, since the September 11 attacks, basic security features such as more security personnel and control of access to train stations, have not been put in place by all commuter rail systems. In addition, the Hudson River tunnels used daily by Amtrak are nearly 100 years old and not likely to withstand an attack.

- **DHS and TSA continue to spend, on average, $9 per air passenger, as compared to only one penny per rail/mass transit rider.** According to the American Public Transportation Association, it will take more than $6 billion to secure mass transit stations across the country.

## Intelligence

GRADE: C+

*"National intelligence is still organized around the collection disciplines of home agencies, not the joint mission. The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to "connect the dots." No one component holds all the relevant information." (9/11 Commission)*

Following 9/11, both the 9/11 Commission and the Joint Inquiry of the House and Senate Intelligence Committees concluded that the U.S. counterterrorism effort leading up to the attack was hampered by a lack of cooperation and information-sharing across agencies, insufficient strategic analysis of al-Qaeda, and shortcomings in our domestic intelligence capabilities.

Congress and the President have carried out many of the recommendations of the 9/11 Commission, such as the creation of a National Counterterrorism Center, the appointment of a high-level Director of National Intelligence, and the development of a national security workforce within the FBI. Unfortunately, these bureaucratic reforms have yet to live up to expectations. Moreover, new intelligence technology projects have routinely been overdue and over-budget.

- **The National Counterterrorism Center (NCTC) has drawn bipartisan criticism for its perceived weakness in turf wars and for merely adding a layer of bureaucracy.** The NCTC was created in 2004, at the recommendation of the 9/11 Commission, to provide a hub for the government's intelligence efforts. However, the fledgling agency is still perceived as having limited effectiveness, and suffers from high turnover and the flight of experienced analysts. In December 2005, the nonprofit successor to the 9/11 Commission gave the U.S. government "D" grades for information-sharing.

- **Intelligence agencies have been hampered in recruiting analysts with native-level language skills, especially in difficult languages such as Arabic.** A prime culprit for the shortfall is the security clearance practices that penalize individuals who lived, studied, or have family members abroad – the same individuals likely to have the cultural understanding necessary to build relationships and gather human intelligence. The New York City Police Department has been a leader in mining the city's multicultural population to improve intelligence capabilities, and federal agencies should learn from its successes.

- **Despite a 68% budget increase from FY 2000 to FY 2005, experts widely acknowledge that the FBI is having severe difficulties shifting its approach from law enforcement to terrorism prevention.** As the FBI's old culture persists, intelligence analysts report that they are short of basic tools like Internet access and they are not respected by special agents from the old guard. Not surprisingly, the FBI has had great difficulty hiring and retaining analysts, with a 2005 report by the DOJ Inspector General revealed that 10% of FBI analysts had left their jobs in each of the preceding three years.

- **Too many efforts to bring intelligence agencies into the digital age have been tales of cost overruns, missed deadlines, and outright failure.** The FBI's chief information technology officer in June 2005 described the agency, which has the lead role in terrorism investigation, as "still paper-based." The FBI recently expended several years and over $100 million in a futile effort to develop a Virtual Case File system that would electronically integrate FBI files to improve case management. The FBI abandoned the program in 2005 after major technical glitches, and continues to struggle along without any integrated database. The agency is now hurrying to develop the Sentinel program to fill this gaping hole.

- **The National Security Agency (NSA) is years behind schedule and hundreds of millions of dollars over budget on its major modernization program, called Trailblazer.** This key program aims to enhance the NSA's capacity for intercepting and sorting telephone calls, e-mails, instant messages, and other signal communications. Unfortunately, the program appears to be developing much more slowly than some of the technology it is intended to filter.

- **In early July, the CIA disbanded the unit devoted to hunting Osama bin Laden, despite the fact that its objective still is not achieved.** Osama bin Laden, arguably America's worst enemy, remains at large despite the CIA's years-long efforts to track him.

## Truck Security

GRADE: C

*"One can envision a scenario where government authorities receive intelligence that a terrorist weapon or terrorists themselves are being smuggled in a particular shipment. Authorities would then want to locate that shipment immediately as well as any other possible shipments that were suspect based on having similar shipment particulars. Currently, authorities would have limited capabilities to locate such shipments quickly." (Congressional Research Service)*

Terrorists have used trucks to attack Americans around the world and on our own soil – in New York City at the World Trade Center in 1993, in Oklahoma City, and at our military compound in Dhahran, Saudi Arabia. Prior to 9/11, the government did very little to track shipments of hazardous materials or perform background checks for any of the drivers who haul these materials.

Today, many of our nation's larger trucking companies have voluntarily placed GPS tracking devices on their trucks. Yet there is no federal requirement that trucks be equipped with GPS technology, and there is no federal center to track truck shipments across the country. Moreover, DHS has stated that it will take at least three more years to run background checks on drivers who transport hazardous materials.

- **DHS has no way to track shipments of hazardous materials.** While Brazil has set up a comprehensive system using GPS technology to track truck shipments of hazardous materials, the United States is lagging far behind with DHS programs testing various tracking stages only in the early testing phases. There have been numerous reports, some in the New York metro area, of trucks carrying gasoline disappearing from parking lots or along their routes. And though local law enforcement usually recovers the truck, had it been hijacked by a terrorist, DHS would have no way of knowing where the truck is.

  Trucks cross the country daily carrying potentially deadly chemicals like ammonium nitrate, chlorine, and cyanide. According to the 1997 Census of Interstate Commerce, 740,000 hazardous materials shipments travel by truck each day in the United States. Approximately 50,000 trips are made daily by gasoline tankers, many of which hold as much fuel as a Boeing 757. These trips often end with a late-night delivery to a deserted gas station.

- **DHS still has not completed full background checks of truck drivers licensed to carry hazardous materials.** DHS initiated a program in 2003 to run background checks on drivers licensed to carry hazardous materials, but this process is not expected to be completed until 2010. The program has been plagued by administrative delays and bureaucratic tangles between state and federal transportation officials.

## Aviation Security

GRADE: B-

*"The DHS Inspector General found that screener training, screening technology, policies and procedures, and management and supervision of screening operations all contributed to observed deficiencies in screener performance. Furthermore, the 9/11 Commission recommended that the TSA give priority attention to implementing technology and procedures for screening passengers for explosives, something not currently done routinely at screening checkpoint." ( Congressional Research Service)*

In the immediate aftermath of the September 11, 2001 terrorist attacks, Congress acted quickly to address the gaping holes in our aviation security system and passed the Aviation and Transportation Security Act, which created the Transportation Security Administration (TSA) and a federalized force of security screeners to inspect passengers and luggage. Post-9/11 security upgrades also included in-flight measures, such as the expansion of the Federal Air Marshal Service (FAMS) and the installation of hardened cockpit doors.

Despite these efforts, weaknesses still exist: a July 2006 Congressional Research Service (CRS) report concludes that airport screener performance is still in need of improvement. The foiled terror plot in London demonstrated the broader concern that TSA still operates primarily through a short term approach. Although it is essential that TSA can react rapidly when necessary, the agency is failing at the long-term task of developing and deploying new technologies that are desperately needed to detect a wide variety of threats.

- **There still are not enough well-trained professional TSA screeners to prevent a weapon from being smuggled on to a flight.** Under current law, TSA cannot employ more than 45,000 screeners at the roughly 500 commercial airports nationwide. The imposition of this cap forced TSA to cut the number of screeners from a previous high of 51,000-52,000 just after 9/11. In addition, a review of screening needs at airports nationwide last year found that the optimal number of screeners is 47,000 based on passenger flow, risk, and projected growth. Because of the cap, TSA is at least 2,000 screeners short of what it needs.

- **Technology to screen passengers for weapons and explosives is years behind where it needs to be.** A Congressional Research Service report, released a day before the recent London flight bomb plot became public, revealed that only 93 detection portals, or "puffers," have been deployed in 34 airports since 2004. (The portal systems cost approximately $160,000 each.) In fiscal year 2006, Congress gave TSA $4.6 billion specifically designated for aviation security. But out of that total, only $439 million – less than 10 percent – went to explosive detection on passengers and carry-on bags. Much of the funding went towards checkpoint screening and the TSA's federalized screening force.

- **According to the GAO and the DHS Inspector General, even though more than half of its annual budget of almost $6 billion is devoted to baggage and passenger screening (including screeners), the TSA has not demonstrably improved the its effort to prevent dangerous objects being smuggled on-board inside checked baggage.** TSA estimates that under current investment levels, installation of Explosive Detection System (EDS) at all US airports will not be completed until 2024. Today, only 51 of the roughly 500 commercial airports in the United States either have or are even currently installing some form of advanced in-line baggage screening system. In the entire state of New York, only a few in-line screening systems are being used. The GAO cites a lack of priority and inadequate investment for the delay in implementation, despite the fact that the 9/11 Commission specifically recommended that the TSA expedite installation of inline baggage screening systems.

  EDS is widely acknowledged to be the most efficient means of screening luggage for explosives. Rather than relying on swabbing for traces of explosives, it uses x-ray technology to determine that an explosive material is present. EDS x-rays can also be integrated into airport baggage conveyor systems, reducing crowding and safety hazards in airport lobbies and check-in counters.

- **DHS still has not deployed a comprehensive system to check if a terrorist has bought an airline ticket.** While $130 million has been spent on the Secure Flight program—a system that would match airline passengers against terrorist watch lists—the Government Accountability Office (GAO) reports that it faces considerable management and oversight challenges. The TSA suspended the program in March due to security concerns.

  *This is the second time since 9/11 that DHS has had to scrap a plan to check passenger names against a terrorist watch list.* Secure Flight is the successor to the controversial, and never-deployed, CAPPS II, which was widely criticized by privacy advocates and Congress for being too intrusive in to the passenger data it planned to collect.

- **Passenger manifests of international flights are only checked after the flight leaves the airport, meaning DHS cannot know if a terrorist is aboard a United States-bound flight until the flight is already in the air.** Current law requires airlines to transmit their international flight manifests to DHS within 15 minutes before take-off so the manifests can be checked against the terrorist watch list.

  In December 2004, recognizing the potential for terrorist exploitation, Congress enacted a requirement that DHS—within 60 days—offer new regulations mandating that airlines transmit their international flight manifests before an international flight takes off. Secretary Chertoff even met with European security officials in May 2005 to negotiate a new agreement. However, the Administration has failed to reach an agreement with European authorities, DHS has not issued the guidelines that are now 18 months overdue, and international passenger lists are still not checked before the flight takes off.

- **TSA has done very little to ensure that foreign airports are complying with international security standards, and has made a mediocre effort to coordinate with foreign governments. Currently, TSA only has 21 inspectors stationed abroad as security coordinators and points-of-contact for foreign government officials.** These Transportation Security Administration Representatives (TSARs) are stationed around the world to "promote alignment and consistency, conduct airport assessments, consult with the host country on aviation security matters, serve as on-site coordinators for TSA in the event of a terrorist attack, and ensure air carriers are complying with U.S. regulations." However, there are not nearly enough TSARs deployed worldwide to make certain that foreign airports are in compliance and operating at an appropriate level of security.

- **Many countries use bomb-detection equipment for checked baggage that does not meet U.S. standards, according to a report last year by the Homeland Security Department.** Last week, a college student accidentally brought a stick of dynamite onto Continental Airlines flight from Argentina to Houston, and the explosive was not detected until his arrival on U.S. soil. DHS has not been nearly aggressive enough in inspecting foreign airports. In September 2004, TSA officers detained Shaun Marshall, a medic for defense contractor DynCorp Inc., at John F. Kennedy International Airport after he successfully carried a "Soviet V429E projectile point detonating fuse and a 23mm Society military full-round surface-to-air and air-to-air cartridge" on board a flight.

- **TSA still only screens 10 to 15% of the 6 billion pounds of air cargo that travels on passenger flights every year.** About 27% of domestic air cargo travels aboard passenger aircraft within the United States, while 45% of international cargo to and from the United States is carried aboard passenger aircraft. TSA believes that cargo is either likely to become, or already is, the primary aviation target for terrorists in the short term. It has been reported that TSA considers the likelihood of a terrorist bombing of a passenger airplane to be between 35% and 65% based on 2002 intelligence reports.

  Despite releasing interim rules nearly two years ago, DHS has yet to issue final, enforceable security standards for air cargo security. According to the TSA, only one-third of air carriers and indirect air carriers are participating in the voluntary DHS security programs to vet cargo destined for passenger aircraft.

- **There is no standard, tamper-proof, biometric identification card for airport workers which would prevent a terrorist from sneaking on board a flight without a boarding pass, or breaking into secure areas.** TSA recently announced it planned to roll out a biometric identification card for seaport workers later this year, but there is no plan to extend the Transportation Worker Identification Credential (TWIC) program to the aviation sector any time soon.

  TWIC is a tamper-resistant credential that contains biometric information about the holder which renders the card useless to anyone other than the rightful owner. Using this biometric data, each transportation facility can verify the identity of a worker and help prevent unauthorized individuals from accessing secure areas. Airports can employ thousands of people, and it is essential that there be a standard, tamper-proof identification card to keep terrorists out of sensitive and secure airports.

  The program was originally scheduled to be deployed years ago at ports, airports, and transportation facilities across the country, but it has been repeatedly delayed due to political wrangling and mismanagement by DHS.

- **There is still no comprehensive system to protect commercial aircraft from shoulder-fired missiles, called MANPADS.** It is estimated that there are currently over half a million MANPADS weapons worldwide. Aircraft during takeoff and landing are also vulnerable to attacks with .50 caliber rifles, powerful sniper weapons that are military-grade but can be purchased by civilians in the United States. Enlarging the safety perimeter around all airports is not a foolproof solution, as most aircraft fly within small arms firing range for approximately 25 miles, but perimeter expansion would be a good first step towards protecting against such a threat. TSA has conducted vulnerability assessments regarding MANPADS, but as of yet no airports have made a significant effort to acquire more land to extend their security perimeters.

  According to a recent RAND Corporation study, laser jamming technology to counter MANPADS will soon be readily deployable on-board aircraft, but the major DHS program to develop and test the project is still in the early stages.

  The United States must engage in more international cooperation to directly target the spread of small arms on the international black market. More specific approaches—such as buyback programs, improved security at transportation hubs worldwide, and assistance to nations to destroy surplus MANPADS—should be implemented as soon as possible.

## Detection Devices

GRADE: F

*"You have to have a long-term strategy and a short- to medium-term strategy. What we have been doing is shifting resources back and forth between those two goals. The result of that is we are not making the best progress in either one." (Stephen J. McHale, former deputy administrator of the T.S.A)*

Before the 9/11 attacks, research and development in to advanced bomb detection technologies was limited, focusing primarily on keeping metal objects off of airplanes. When DHS was created, the Department included a Science and Technology directorate to oversee critical technological development. However, in all areas of security, progress has been dangerously slow, with advanced explosive detectors for mass transit systems still on the drawing board and nuclear container scanners at ports more likely to pick up kitty litter and lemons than a nuclear device.

- **To date, there is still no technology available that can be deployed at a rail station or on a car that can warn authorities and passengers of the presence of a nuclear, chemical, radiological, or explosive device.** To protect mass transit systems, over the past three years, DHS has tested bomb-detecting technology at an Amtrak station outside Washington and a subway station used by 15,000 New Jersey commuters to enter Manhattan. However, these programs are still in the early testing phases and the results have been decidedly mixed.

- **In addition, technology meant to be deployed at major train stations and at subways entrances has proven ineffective and too slow.**

- **Most of DHS and TSA's research has focused far more on detecting explosives in baggage rather than testing passengers.** TSA estimates that under current investment levels, installation of Explosive Detection System (EDS) for checked baggage at all US airports will not be completed until 2024.

- According to Steven Flynn, a port security expert at the Council of Foreign Relations, "the radiation-detection technology currently used in the world's ports by the Coast Guard and Customs and Border Protection Agency is not adequately capable of detecting a nuclear weapon or a lightly shielded dirty bomb. This is because nuclear weapons are extremely well-shielded and give off very little radioactivity. If terrorists obtained a dirty bomb and put it in a box lined with lead, it's unlikely radiation sensors would detect the bomb's low levels of radioactivity."

## Spread of Nuclear Materials

GRADE: C-

*"We still do not have a maximum effort against the most urgent threat to the American people." (Thomas H. Kean and Lee Hamilton)*

Since 9/11, the most terrifying attack on the minds of Americans and homeland security experts is the possibility of nuclear device being detonated in major city. After the Cold War, countless stockpiles of unused Russian nuclear weapons were left unprotected and vulnerable to theft by terrorists or resale by rogue states like Iran and North Korea. The United States government's primary program to recover and secure these weapons, known as Nunn-Lugar, has so far collected half of the known nuclear weapons stockpiles. However, the Bush Administration has cut funding for this critical program even though its vital task has not been completed.

- **9/11 Commission Chairman Thomas Kean estimated that 500,000 lives could be lost in the explosion of a nuclear weapon in Manhattan.** Kean has warned, "These are the weapons Osama Bin Laden has promised to obtain and use ... such a possibility must be elevated above all other problems of national security." A March 2006 Council on Foreign Relations report similarly concluded that the "threat of a nuclear attack by terrorists has never been greater" and the United States has yet to make prevention a true priority.

- **Due to slashed spending on the Nuclear Cooperative Threat Reduction (Nunn-Lugar) program under President Bush, less nuclear material was secured from 2001 to 2005 than in the four years before 9/11.** It is well known that there is a busy black market in nuclear materials from the former Soviet Union and other areas, and that terrorist organizations have tried to obtain such materials. The need to secure nuclear materials grows more urgent as weapons technology spreads to states with mixed or poor records on fighting terrorism, like Pakistan and North Korea.

- **According to the leaders of the 9/11 Commission, 14 years after the fall of Communism, only half of Russia's nuclear materials have been neutralized under a joint US-Russian agreement to reduce nuclear weaponry. The other half remains at risk of falling into the hands of terrorist groups or rogue nations.**

- **The United States and the world have not taken adequate steps to contain supplies of highly enriched uranium and the spread of enrichment technology.** Too often, these stores of existing weapons-grade uranium are poorly tracked, controlled, and guarded. Pakistan's President Musharraf, in particular, has created cause for concern by expressing disbelief that terrorists can or wish to use nuclear technology.

*"Federal resources are scarce in proportion to the number of potential targets. Congress and the Administration must set priorities based on the risk, vulnerability, and consequences of an attack on a given site." (9/11 Public Discourse Project, successor to the 9/11 Commission)*

## First Responder Grants

GRADE: F

Since DHS was created in the wake of 9/11, the agency has issued billions of dollars in grants to first responders and high-threat areas to help them protect against and respond to terrorist attacks. Unfortunately, these critical funds have been terribly mismanaged and have not been given to the areas that face the greatest risk and threat.

- **The President's FY2007 budget cut funding for programs designed to assist state and local law enforcement agencies by more than $1 billion compared to FY2006**. The Firefighters Grant Program was cut by 50 percent and the National Domestic Preparedness Consortium, which trains first responders, was cut by 66 percent. In addition, the President's 2007 budget requested no funding to enhance interoperable communications.

- **DHS's process to give out first responder grants is in disarray.** Just days after cutting New York City's high threat preparedness funding by 40 percent, DHS released a report that found that New York City did not meet federal disaster guidelines in several critical emergency preparedness areas.

- In June, the Department of Homeland Security released funding allocations for its major state and local grant programs, including the State Homeland Security Grant Program (SHSP), and the High Threat Urban Areas Program (UASI) that gives money only to high threat urban areas.

- Funding for New York State and New York City was cut significantly from FY2005 to FY2006. For UASI, the high threat money actually given out by the program was cut from $829.7 million in FY2005 to $710.6 million for FY2006, or a 14 percent drop overall. However, New York City's allocation was slashed by 40 percent, from $207.6 million in FY2005 to only $124.5 million. In FY2005, New York City received 25 percent of the high threat funding, but for FY2006, New York City will only receive18 percent of the funding to meet the outstanding needs identified by DHS itself.

- In addition, according to a new audit from the DHS Inspector General's office, **dozens of questionable locations around the country are counted as terrorist targets**, including a petting zoo in Woodville Alabama; a Mule Day Parade in Columbia, Tennessee; and the Amish Country Popcorn company, which has five employees in Berne Indiana. The same report found that Indiana had 50 percent more terrorist targets listed than New York (5,687 targets) and twice as many as California (3,212 targets). The DHS inspector general found that the Department relied on this dysfunctional database when making critical funding decisions.

## Nuclear Plant Security

GRADE: B+

*"Protection of nuclear power plants from land-based assaults, deliberate aircraft crashes, and other terrorist acts has been a heightened national priority since the attacks of September 11, 2001. The NRC has strengthened its regulations on nuclear reactor security, but critics contend that implementation by the industry has been too slow and that further measures are needed." (CRS)*

For each nuclear energy facility in the United States, the Nuclear Regulatory Commission (NRC) sets security standards that define a level of attack that the facility must be able to repel, known as the Design Basis Threat (DBT), and conducts regular inspections. While there is still room for improvement, nuclear plants have long been strictly regulated and improvements are ongoing. Remaining areas of concern are the enforcement of existing security standards and preparedness for nuclear incidents.

- **A recent GAO report found that the process used to revise the DBT security standards was overly influenced by the views of the nuclear industry.** In addition, experts have criticized the new standards because they will not require plants to meet a threat equal to that posed by the 9/11 terrorist group. In other words, nuclear plants will not be expected to fend off a coordinated attack by 19 individuals, even though we know that terrorists are capable of this type of organization.

- **Moreover, the GAO's review of a sample of NRC inspection records found that nuclear plants frequently are not meeting security standards.** The GAO study found that there were security problems or items needing correction uncovered in 12 of 18 baseline inspections (in which the NRC checks a plant's readiness and controls) and 4 of 9 force-on-force inspections (in which the plant defends against a simulated attack). Although force-on-force inspections are critically important in uncovering these problems, NRC had conducted them at just one-third of plants by the time of the GAO's review.

- **The risks of terrorist attacks against nuclear plants are too dire to be ignored.** For example, the Indian Point nuclear power plant is situated just 35 miles north of midtown Manhattan. A 2004 report by the Union of Concerned Scientists found that, in a worst-case scenario attack against Indian Point, up to 44,000 people could be killed by a massive and lethal release of radiation.

- **Current disaster planning may not accurately reflect the risks of nuclear attack.** Every nuclear plant is surrounded by an Emergency Planning Zone of only 10 miles, within which plants must install sirens and conduct evacuation drills, and residents can get supplies of iodine pills to prevent radiation contamination. Since 9/11, there have been calls to extend the Emergency Planning Zone to a larger distance such as 50 miles, to better reflect the reach of a nuclear incident. A 50-mile perimeter would compel Indian Point to include Manhattan in its emergency planning.

## Biosecurity

GRADE: C+

*"The U.S. does not yet have a coherent biodefense strategy ... that takes into account the full spectrum of possible bioweapons agents, including engineered threats," (Tara O'Toole, a co-founder of the University of Pittsburgh's Center for Biosecurity)*

Though the United States has never been hit with chemical or biological attack, the attacks of 9/11 showed the country that terrorists will use any means necessary to inflict death and destruction. DHS and the Department of Health and Human Services administer a comprehensive program to protect the country from a biological attack by creating stockpiles of medicine and antidotes. Unfortunately, the effort is understaffed, underfunded, and poorly managed.

- **The Administration's primary program to protect Americans from a biological attack is in shambles.** Two years after Congress created "Project Bioshield", which was supposed to be a comprehensive national stockpile of drugs and other measures to counter the effects of biological and radiological weapons, the effort has been plagued by delays and bureaucratic fumbles and the Administration has not fully implemented its mandate.

  According to the Center for Biosecurity at the University of Pittsburgh, the Department of Health and Human Services simply lacks the personnel to manage the $5.6 billion program efficiently and estimated that it needs at least 100 more employees, on top of only 40 people currently working on the project, to get the job done.

## Chemical Plant Security

GRADE: D

*"I am aware of no other category of potential terrorist targets that presents as great a danger." (Richard Falkenrath, former top Homeland Security adviser to President Bush)*

Chemical facilities across the country produce and process some of the most dangerous materials known to man, and many of these plants are located near densely populated areas. Some major chemical companies have voluntarily instituted security improvements. However, many plants remain vulnerable and there is a serious need for greater federal leadership in this area.

- **Five years after 9/11, DHS still has not implemented enforceable national standards to secure the chemical plants that house some of the most dangerous materials on earth.** DHS has displayed a disturbing pattern of negligence and a lack of urgency towards upgrading security standards. A DHS report for developing a strategy for protecting the nation's infrastructure, including a plan to protect the chemical plant industry, was long overdue. Finally released in June 2006, the DHS report titled, "National Infrastructure Protection Plan," consists only of vague guidelines.

  The United States is home to approximately 15,000 chemical plants that have hazardous chemicals on site, and the GAO recently identified over 100 plants nationwide that if attacked would threaten at least one million Americans. The nation's chemical infrastructure is believed to be a likely terrorist target because of its potential for causing widespread harm. Both the 9/11 Commission Report and the FBI's National Infrastructure Protection Center (now in the Department of Homeland Security) have warned that terrorist operatives may attempt to launch conventional attacks against the U.S. chemical-industrial infrastructure.

## Cyber Security

GRADE: C-

*"However, despite growing concerns for national security, computer vulnerabilities persist, the number of computer attacks reported by industry and government has increased yearly, and federal agencies have, for the past three years, come under criticism for the poor effectiveness of their computer security programs," (Congressional Research Service)*

Terrorist organizations like Al Qaeda, Hamas and Hezbollah, who previously used the Internet for fundraising, communication and propaganda, are now suspected of using the Internet to develop advanced cyber weapons to attack U.S. systems. After 9/11, the Administration issued cyber security standards for federal networks and created the position of Cyber Security Czar. However, the standards remain unfulfilled and the position, more than a year after being created, is still vacant.

- **After a year-long vacancy, DHS still has no Cyber Security Czar to oversee the security of America's cyberspace.** Richard Clarke, a former cyber-security adviser to Presidents Bush and Clinton, has said that it is critical that President Bush nominate an individual to serve as cyber security czar for Homeland Security. Recent disastrous failures at the Departments of Veterans Affairs, Agriculture, Energy, State, Defense, Health and Human Services, the Federal Trade Commission, and Federal Bureau of Investigation have put the personal information of millions of Americans at risk, and the electronic security of our nation in doubt. The personal information of veterans, soldiers, nuclear weapons workers at the Department of Energy, and employees across the government has been disclosed, as has the medical records of ordinary Americans and the vital military secrets of the U.S. military.

- **President Bush took the lead in developing a National Strategy to Secure Cyberspace, but plans are not enough.** The strategy released in February 2003 sets out specific executive branch actions that will improve the security of our homeland cyberspace, but too many of these promises are still unfulfilled.

- **Though the President pledged to secure federal wireless local area networks, more than two years after the President released his strategy, a 2005 GAO report concluded that federal agencies had far to go in implementing key security elements for wireless networks.** At the six agencies tested, the wireless networks in use were not secure and the GAO was able to detect activities from outside the buildings. Nine federal agencies had not even issued policies regarding wireless networks. Eighteen of 24 federal agencies had no wireless security training for employees and contractors.